「パス構築・パス検証」クライアントサンプル実装

CryptoAPI 版

取扱説明書



2003 年 3 月

情報処理振興事業協会

1 マイクロソフト CryptoAPI サンプル実装取り扱い説明.. 1
1.1 概要.. 1
1.1.1 テストプログラムの内容.. 1
1.1.2 稼働環境.. 2
1.1.3 署名テストプログラム 3
1.1.4 署名検証テストプログラム 6

1 マイクロソフト CryptoAPI サンプル実装取り扱い説明

1.1 概要

マイクロソフト Windows の開発環境においては、セキュリティのプラットホームとして CryptoAPI が用意されている。CryptoAPI を利用することにより、各プログラムは、証明書を操作することできる。

CryptoAPI を利用してブリッジ CA モデルの PKI 環境においてデジタル署名および署名検証を適切に処理するサンプル実装を開発した。

署名テストプログラム：pkiicsig

署名検証テストプログラム：pkiicver

1.1.1 テストプログラムの内容

CryptoAPI サンプル実装は以下のようなファイルにより構成されます。これらを適当なディレクトリに展開します。

表 1-1 配布ファイルの一覧

	ファイル名	役割
1	readme.txt	リリースノート
2	pkiic.dat	設定ファイル（アンサポート）
3	pkiicsig.exe	署名テストプログラム
4	pkiicver.exe	署名検証テストプログラム
5	aicrypto.dll	署名検証テストプログラム用のダイナミックリンクライブラリ
6	aipass.dll	署名検証テストプログラム用のダイナミックリンクライブラリ
7	cmapi_o.dll	署名検証テストプログラム用のダイナミックリンクライブラリ
8	cmlasn_o.dll	署名検証テストプログラム用のダイナミックリンクライブラリ
9	libCert_o.dll	署名検証テストプログラム用のダイナミックリンクライブラリ
10	libCtil_o.dll	署名検証テストプログラム用のダイナミックリンクライブラリ
11	ldapsdk.dll	署名検証テストプログラム用のダイナミックリンクライブラリ
12	pkiicrp.dll	署名検証テストプログラム用のダイナミックリンクライブラリ
13	sm_aiCrypto.dll	署名検証テストプログラム用のダイナミックリンクライブラリ
14	snacc_o.dll	署名検証テストプログラム用のダイナミックリンクライブラリ
15	srlapi_o.dll	署名検証テストプログラム用のダイナミックリンクライブラリ

1.1.2 稼働環境

CryptoAPI サンプル実装は以下の条件をみたす環境にて稼動します。

- OS：Microsoft Windows 2000、Microsoft Windows XP
- Internet Explorer バージョン 5 がインストールされていること

1.1.3 署名テストプログラム

(1) 機能説明

デジタル署名処理を実行する。
指定された秘密鍵及びそれに関連する証明書を利用して、対象データに署名処理を実行する。対象データが指定されていない場合は、任意のデータをテスト用にセットして、署名処理を行う。
署名処理結果は、特に指定が無い場合は標準出力に出力される。失敗の場合は失敗理由もあわせて出力する。署名されたデータは、署名データとして、`元のファイル名.p7m'として保存される。

(2) 名前

pkiicsig

(3) コマンドラインの書式

pkiicsig [オプション] cert<1> cert<2 >...cert<n>

(4) コマンドラインオプション

以下の引数を指定する。

cert<1> cert<2 >...cert<n>

署名処理に使用する秘密鍵に関連する証明書を任意数指定可能。複数指定する場合は、各引数間を空白（スペース）で区切る。-c により任意のクレデンシャルが指定されている場合は、何も指定しなくてもよい。ここで指定する証明書のデータ形式は、DER 形式とする。

表 1-2 pkiicsig コマンドオプション一覧

<table>
<tr><th>オプション</th><th>オプションの引数</th><th>必須項目</th><th>説明</th></tr>
<tr><td>-v</td><td>なし</td><td>－</td><td>このテストプログラムが基づいているテストプログラム仕様のバージョン番号を表示する。</td></tr>
<tr><td>-m</td><td>SHA1 | MD5</td><td>－</td><td>メッセージダイジェスト生成アルゴリズムをフラグで指定する。省略可能。省略時のデフォルト値は、SHA1。</td></tr>
<tr><td>-c</td><td>File 名</td><td>○</td><td>署名処理に使用する秘密鍵とそれに関連する証明書を含んだクレデンシャルファイルを指定する。クレデンシャルファイルは、PKCS#12 フォーマットもしくは、各実装依存の独自フォーマットとする。初期値が指定されている場合、-c オプションを優先する。</td></tr>
<tr><td>-d</td><td>File 名</td><td rowspan="2">○</td><td>署名処理を行う対象となるデータファイルを指定する。ファイルに格納されているデータ形式は問わない。</td></tr>
<tr><td>-f</td><td>Path 名</td><td>署名処理を行う対象となるデータファイルが格納されているフォルダ/ディレクトリを指定する。このオプションによりデータが指定される場合は、path で指定されたフォルダ/ディレクトリ以下全てのファイルが署名対象となる。パス内のファイルに格納されているデータ形式は問わない。</td></tr>
<tr><td>-o</td><td>File 名</td><td>－</td><td>署名処理済み（署名結果）ファイル名を指定する。省略可能。省略時のデフォルト値は、`元のデータファイル名.p7m’。</td></tr>
<tr><td>-p</td><td>Passphrase</td><td>○</td><td>-k で指定された署名を行うために使用する秘密鍵に対するパスフレーズを入力する。</td></tr>
</table>

○：指定必須　－：指定任意。

(5) 使用例

秘密鍵 mysert.p12、を使用して、ファイル test.txt に署名処理を行う。

```
gpksign –c mysert.p12 –d test.txt

OK/NG output: test.p7m
```

(6) 終了ステータス

以下の終了ステータスが返される。

0	正常終了
<0	内部エラー（システムエラー）が発生した。

1.1.4 署名検証テストプログラム

(1) 機能説明

指定された証明書及びポリシーを利用して、対象データの署名検証を行う。上記引数の他に、任意の設定ファイル等による初期値指定方法を備えなければならない。
署名検証結果は、標準出力に出力される。失敗の場合は失敗理由もあわせて出力する。

(2) 名前

pkiicver

(3) コマンドラインの書式

pkiicver [オプション] ipcy<1> ipcy<2 > … ipcy<n>

(4) コマンドラインオプション

以下の引数が指定できる。

ipcy<1> ipcy<2 > … ipcy<n>

initial-policy-set を任意数指定することができる。複数指定する場合は、各引数間を空白（スペース）で区切る。省略可能。省略時は、NULL を示す。規定値として、以下の値が使用可能である。

"ANY" ：全てのポリシーを受け入れる場合(any-policy)。

-ie オプションが有効な場合は、引数として NULL 以外の値を指定しなければならない。

表 1-3 pkiicver コマンドオプション一覧

オプション	オプションの引数	必須項目	説明
-v	なし	―	このテストプログラムが基づいているテストプログラム仕様のバージョン番号を表示する。実装必須。
-d	File 名	△	署名検証検証を行う対象となるデータファイルを指定する。
-f	Path 名	○	コマンドラインに指定されているファイルが格納されているフォルダ/ディレクトリを指定する。
-c	File 名	△	検証対象証明書ファイル（der 形式）を指定する。-c オプションが指定された場合は、署名検証を行わず、証明書検証（証明書パス構築・検証）のみを行う。
-t	File 名	○	署名･証明書検証側トラストアンカーの自己署名証明書ファイル（der 形式）を指定する。
-P	[File 名]	―	中間 CA の証明書ファイルを指定する。中間 CA の証明書ファイルが１つも無い場合は、「-P」のみを与える。ファイルを複数指定する場合は、コロン「:」で区切る。このオプションが指定された場合はオフラインモードで動作し、リポジトリや OCSP への問い合わせは行わない。※
-ip	なし	―	initial-policy-mapping-inhibit フラグの有効/無効を指定する。-ip オプションがある場合、有効となる。
-ie	なし	―	initial-explicit-policy フラグの有効/無効を指定する。-ie オプションがある場合、有効となる。その場合、コマンド引数（initial-policy-set を指定する）は、NULL 以外でなければならない。
-ia	なし	―	initial-any-policy-inhibit フラグの有効/無効を指定する。-ia オプションがある場合、有効となる。
-l	Host 名	―	LDAP サーバのホストとポート番号を「IP アドレス:ポート番号」もしくは「FQDN:ポート番号」の形式で指定する。

○：実装必須 △：いずれかが必須 ―：指定装任意。

※各 CA が発行する CRL/ARL については、各 CA 証明書（トラストアンカー、中間 CA 証明書）のファイル名の拡張子が `crl` あるいは `arl` となっているものを読み込む。これらのファイルは全て-f で指定されたパス配下にあるものとする。

(5) 使用例

＜例 1＞

/project/date 配下にある target.1.1.1.crt を検証対象証明書ファイルとし、trust.1.1.1.crt をトラストアンカー証明書ファイルとして、証明書リポジトリとして ldap.gpki.go.jp を使用し、証明書検証をオンラインモードで行う。

pkiicver –f /project/data –c target.1.1.1.crt –t trust.1.1.1.crt –l ldap.gpki.go.jp:389

出力

有効な証明書です

＜例 2＞

/project/date 配下にある target.1.1.1crt を検証対象証明書ファイルとし、trust.1.1.1.crt をトラストアンカー証明書ファイルとして、証明書検証のみをオフラインモードで行う。

intermediate.1.1.1.crt 及び intermediate.1.1.2.crt を中間 CA の証明書ファイルとし、トラストアンカーや中間 CA の CRL/ARL については、それぞれのファイル名の拡張子が crl または arl となっているファイルを参照する。

pkiicver –f /project/data –c target.1.1.1.crt –t trust.1.1.1.crt –P intermediate.1.1.1.crt:intermediate.1.1.2.crt

出力

有効な証明書です

(6) 終了ステータス

以下の終了ステータスが返される。

0	正常終了
>0	検証エラーが発生した。
<0	内部エラー（システムエラー）が発生した。

(7) 検証エラー

表 1-4 検証エラー診断値

診断値	説明
証明書検証の基本的なエラー	
8	信頼する証明書が自己署名でありません
9	内容が正しくないデータです
12	公開鍵のパラメータがありません
13	DN が正しくありません
14	署名用鍵ではありません
19	原因を特定できないエラーです。
20	リポジトリに見つかりませんでした
21	証明書パスを確認できません。
22	拡張エラーがありません
23	証明書の失効情報が確認できませんでした
27	信頼できる証明書がありません。
28	信頼している証明書の読み込みに失敗しました
29	信頼している証明書はまだ有効ではありません
30	信頼している証明書は有効期限が切れています
31	信頼している証明書の署名が不正です
32	不明なエンコードタイプです。
33	オブジェクトのロケーションが不正です
34	トークンがサポートしていない署名アルゴリズムです
35	オブジェクトの署名が不正です
36	署名処理が失敗しました
37	デフォルトのトークンライブラリの初期化に失敗しました
ディレクトリ関連のエラー	
42	ディレクトリアクセス機能が使用できませんでした。
43	ディレクトリアクセスのための初期化が失敗しました。
44	ディレクトリへの接続に失敗しました。
45	LDAP のバインド処理が失敗しました。
46	LDAP の検索処理が失敗しました。
47	LDAP の検索処理が失敗しました。
48	LDAP の検索処理が失敗しました。

49	条件に合うものが見つかりませんでした
パス構築、パス検証のエラー	
100	証明書のアルゴリズムの指定が一致していません
101	証明書の署名が不正です。
102	証明書はまだ有効ではありません。
103	期限切れです。
104	証明書パス中の名前が正しくつながっていません
105	証明書のパス長が制限を越えました
106	不正な CA の証明書です
107	基本制約に違反があります
108	名前制約に違反があります
109	ポリシー制約に違反があります
110	ポリシーマッピングが正しくありません
111	証明書のポリシーがが正しくありません
112	証明書の subject name が正しくありません
113	証明書の用途が正しくありません
114	証明書の別名の中に認識できない形式があります
115	証明書の別名が不正です
116	重要と指定された認識できない拡張項目があります
117	この CA が発行した失効リストが見つかりません
118	失効リストの署名アルゴリズムが合いません
119	失効リストの署名が正しくありません
120	最新の失効リストがありません
121	証明書は失効しています(理由不明)
122	証明書の公開鍵の安全性に問題があります
123	証明書は失効しています(内容に変更があります)
124	証明書は失効しています(更新されています)
125	証明書は失効しています(もう使われません)
126	証明書は失効しています(一時的に停止しています)
127	認識できない重要と指定された失効リストの拡張があります
128	認識できない重要と指定された失効リストエントリの拡張があります
129	認識できない重要と指定されたキー使用目的の拡張があります
130	no CTIL supports the signature algorithm on this cert
131	no CTIL supports the signature algorithm on this CRL
132	重要と指定された失効理由がチェックできません

133	失効リストは未検証です。
134	正しくない失効リストです
138	正しくない間接失効リストです
139	失効リストのパスが見つかりません
140	失効リストのパスが正しくありません
141	サポートしていないクリティカルな名前制約の形式です
142	不正なクリティカルな拡張鍵使用法です
143	subject DN missing from trusted cert
144	信頼できる証明書は自己署名の証明書ではありません
145	信頼できる証明書には署名用の鍵がありません
146	信頼できる証明書にアルゴリズムパラメータがありません
180	証明書は失効しています（OCSP)
181	OCSP サーバから失効情報が取り出せませんでした

(8) 設定ファイル pkiic.dat

キー	説明（太字は配布ファイルでの値）
[PkiiCRP]セクション	
ShowStatus	true:「検証中です...」を表示する。**false**:しない
ShowVerifyResult	検証結果の表示 **0**:しない 1: 問題のある証明書なら 2:する
[PkiiCVerify] セクション	
UseCAPIVerification	true:CryptoAPI の Certificate Chain Verification Functions で検証する **false**:オリジナルの Revocation Provider で検証する
CRPRegist	**true**:プログラム起動直後に Revocation Provider を登録する false:登録しない
CRPUnregist	**true**:プログラム終了直前に Revocation Provider を削除する false:登録しない
CRProvider<n>	登録する Revocation Provider の DLL ファイル名 **1; pkiicrp.dll**
DiffExpvalue	テストデータのディレクトリの expvalue.dat に格納されている期待値とことなる場合、ディレクトリ名をしたいされたファイルに格納

(9) 証明書検証機構について

本実装では証明書のパス構築、パス検証の処理方式を以下の 2 つより選択可能です。

- CryptoAPI 標準
- 本プロジェクトで開発したオリジナル

CryptoAPI 標準の機能では、initial-policy-mapping-inhibit、initial-explicit-policy、initial-any-policy-inhibit や受け入れポリシーなどポリシーに関連する初期パラメータを指定した上でのパス検証が不可能ですが、オリジナルの証明書検証機構ではこれを可能としています。

この 2 つは設定ファイルの「UseCAPIVerification」キーにより選択します。

(10) 注意事項

本テストプログラムは同時に複数起動することはできません。